

App. No. 10/779,382
Amendment Dated: July 3, 2007
Reply to Office Action of March 12, 2007

RECEIVED
CENTRAL FAX CENTER

JUL 03 2007

REMARKS/ARGUMENTS

The Office Action mailed March 12, 2007 has been received and the Examiner's comments carefully reviewed. Claims 1-20 are rejected. Claims 11 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Carro (US 2004/0054906). Claims 1-10, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mache (US 2001/0002929). Claims 12-15 and 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carro in view of Mache. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Carro in view of Mache and further in view of Ellison et al. (US 2004/002501). Claims 1, 8, 10, 11 and 12 have been amended. No new matter has been added. The Applicants respectfully submit the following for consideration.

Claim Objections

Claim 1, 10-12 and 14 were objected to because of informalities. In response, Claims 1, 10-12 and 14 have been amended to correct the informalities.

Claim Rejections

Claim 1-10 and 19 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. With regard to Claim 1, the Office Action states that "assembling the next frame such that the data block and the HMAC value appear before the hash key in the frame transmission" is confusing as it cannot be ascertained because the specification fails to disclose how the HMAC value appears before the hash key." The Applicants respectfully

App. No. 10/779,382

Amendment Dated: July 3, 2007

Reply to Office Action of March 12, 2007

disagree. Figure 8 clearly shows the HMAC value before the HMAC key in the frames. Additionally, lines 20-25 of the Applicants specification states "Since the HMAC key is received further along in the time line for transmission than the HMAC value, the late arrival of the HMAC key is not very helpful since the remainder of the transmission is gone. The window of opportunity for a replay attack is very small if it exists at all, since the client device can use its own internal clock and information from the last received frame to close the window between that last frame and the next one expected."

The Office Action also states that "Claim 1, the phrase retrieving a data block that is scheduled for transmission in the next frame" is confusing. In response, the Applicants have changed the term "receiving" to "obtaining."

The Office Action also states that the phrase "selecting a hash key that is associated with the data block" is confusing, because in claim 1, line 3 the applicant refers to a single data block, in claim 1, line 6 the applicant refers to multiple data blocks, therefore it is unclear as to which "data block: applicant referring to in the claimed invention." The Applicants have amended Claim 1 to clarify that a frame has multiple blocks and the data block is one of the blocks.

With regard to Claim 8, the Office Action states that "wherein periodically signing the datum comprises at least one of signing the datum for every frame, and signing the datum over an interval that does not correspond to every frame" the claimed invention as claimed is confusing as the specification failed to disclose how the datum is signed for every frame and then signed the datum not corresponding to every frame. No further merit will be giving to this

App. No. 10/779,382
Amendment Dated: July 3, 2007
Reply to Office Action of March 12, 2007

claim." The Applicants respectfully disagree but have amended Claim 8 to specify that the datum is signed for every frame.

With regard to Claim 19, The Office Action states that " a means for recording the other hash key when the frame is accepted, wherein the other hash key is utilized for verification of subsequently received transmission frames" the term "recording the other hash" cannot be ascertained because the specification fails to disclose how the recording of the other hash is being done." The Applicants respectfully disagree. The Applicants specification includes means for "recording the other hash." For example, FIGURE 4 includes RAM, ROM, and other storage as well as a processing unit that may be used in recording.

The Applicants respectfully request the rejections be withdrawn.

Claim Rejections

Claims 11 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Carro. Regarding claim 11 and 16 the Office Action states that Carro discloses "retrieving signed data from a frame (para. 0032, lines 7-9); verifying an RSA signature associated with the RSA signed datum from the frame (para. 0032, lines 9-12); storing a hash key that is associated with the frame when the RSA signature is verified (the prior art discloses the hash key of the hash function received is being computed to obtain the hash value, therefore, the hash key must have be stored before it can use to decode the hash value (0032, lines 13-18); retrieving another hash key and an HMAC value from the frame; verifying the other hash key (a frame is a data packet of fixed variable, and since every frame transmitted is hashed in iteration sequence each frame

App. No. 10/779,382
Amendment Dated: July 3, 2007
Reply to Office Action of March 12, 2007

must be check and verified for the hash key. the limitation of retrieving another hash key and an HMAC value from the frame and verifying the key is an intrinsic property of the claim invention); verifying the HMAC value with the other hash key (para. 0032, lines 11-20); discarding the frame when at least one of the other hash key and the HMAC value fail verification (para. 0032, lines 21-24); accepting the frame when the other hash key and the HMAC value are successfully verified (para. 0032, lines 18-21)." The Applicants respectfully disagree and present the following for consideration.

Carro is directed at encoding a digital signature of a file into a portion of its filename. At paragraph 20, Carro states that "[t]he invention includes a method for encoding authentication information in the filename of a computer file containing digital data. The method comprises the steps of: computing a hash value of the computer file; computing a digital signature of the computed hash value using a private key of the sender; and encoding the computed digital signature in the filename of the computer file at a predetermined position, or using delimiters."

Paragraph 32 of Carro recites "FIG. 2 illustrates an embodiment of the invention for verifying the authenticity and integrity of a received file 200 that comprises authentication information provided according to the inventive procedure described above with reference to FIG. 1, i.e. by encoding the digital signature of the file 200 into the filename 205. The verification method of this example comprises the steps of: extracting the encoded digital signature 210 from the signed filename 205 of received file 200; recovering the encoded hash value FILE-HASH* 220 of the received file 200 using the public-key 215 of the sender and the encryption algorithm 120 associated with the corresponding private-key 125, and extracted

App. No. 10/779,382

Amendment Dated: July 3, 2007

Reply to Office Action of March 12, 2007

signature 210; computing the hash value FILE-HASH 230 of received file 200 using hash function 225, which is the same hash function 110 used by the sender to compute digital signature 130; comparing the computed hash value FILE-HASH 230 with the decoded hash value FILE-HASH* 220; and, if the computed hash value FILE-HASH 230 and the decoded hash value FILE-HASH* 220 are identical 240, processing the received file 200 as an authentic file 245, else, if the computed hash value FILE-HASH 230 and the decoded hash value FILE-HASH* 220 are different 240, rejecting the received file 200 as being fake or corrupted 250.”

As can be seen, Carro is concerned with hashing a filename in order to create a signed filename. Upon receipt of the digital signature a determination is made as to whether the file is authentic. Among other differences, Carro does not teach the use of different hash keys. Additionally, Carro is not concerned with authenticating frame transmissions and also does not verify a hash key that is obtained from a previous frame. Claim 11 is proposed to be allowable since Carro does not teach the recitations found within Claim 11. Claims 12-16 are proposed to be allowable as they depend from a valid base claim.

Claims 1-10, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mache (US 2001/0002929). Regarding claim 1, the Office Action states that Mache teaches “receiving a data block that is scheduled for transmission in the next frame (para. 0016, lines 1-2; 0037, lines 1-2); selecting a secret key that is associated with the client device for a number of data blocks (para. 0014, lines 3-6; para. 0017, lines 3-5); computing a set of hash keys using the secret key and a count that is associated with time (para. 0031, lines 1-4; para. 0036, lines 1-4); computing an HMAC value for the next frame using the selected hash key (para. 0037, lines 6-7; in the prior art communication are taking place using HMAC for every packets so as to maintain

App. No. 10/779,382

Amendment Dated: July 3, 2007

Reply to Office Action of March 12, 2007

security of the communication exchange); periodically signing and transmitting a datum containing the hash key of an earlier or initial frame with a digital signature key (para. 0037, lines 1-4) Mache discloses all the limitations as disclosed above; except for assembling the next frame such that data block and the HMAC value appear before the hash key in the frame. The general concept of having the HMAC value appear before the hash key as recited in claim 1 is well known in the art. It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Mache to include the use of having the HMAC value appear before the hash key in his advantageous system, as configuring packet header is a common and everyday occurrence throughout the Cryptography and Information Security art and configuring the packet to have the HMAC appear before the hash would have been an obvious matter of design preference, base on such common factor as the secret key must be use to calculate the HMAC; the ordinarily skilled artisan choosing the best method which would most optimize the cost and performance of the device for a particular application at hand, based upon the above noted common design criteria." The Applicants respectfully disagree and present the following. Mache, however, is only disclosing the use of HMAC since it "is hard to break" (paragraph 37). The applicants submit that placing a hash key after the HMAC value is not obvious. Mache in paragraph 37 teaches that the secret key is "exchanged periodically using known secure protocols." HMACS require the use of a shared secret key that needs to remain secret for security purposes. As a result, just sending the secret key in a frame is not done because an attacker can access the exposed secret key. Page 12, lines 14-24 of the Applicants' specification states "HMACs require a shared secret key, which, as described earlier, is inappropriate for broadcast as the secret is exposed to attackers. However, the risk of interception of the shared

App. No. 10/779,382

Amendment Dated: July 3, 2007

Reply to Office Action of March 12, 2007

key can be avoided (provided non-repudiation is not a requirement) by sending the secret key after the block and its corresponding signature, providing two requirements are met. A first requirement is that the recipient must trust that the secret key was chosen by the sender to be used for the specific block, and not by an attacker. A second requirement is that the synchronization mechanism is robust enough that the recipient can know that an attacker would not have been able to prevent the block from being received, capture the secret for that block, and then transmit a fake block with a valid signature using the same secret." The Applicants therefore submit that it is not obvious to include the HMAC value before the hash key. Should the Examiner not agree that Claim 1 is allowable as presented, the Applicants respectfully request the Examiner to point to a reference disclosing such a recitation. Claims 2-10 are proposed to be allowable as they depend from a valid base claim.

Claim 17 seems to be rejected using a similar rationale as Claim 1. Claim 17 recites in part "a scheduler that is arranged to provide data blocks to the server for transmission in a next frame; ... a hashing function in the server that is arranged to compute hash keys for the next frame using the count and a secret key; ... a broadcast processor in the server that is arranged to receive the hash keys, HMAC values, and the data blocks, and organize the next frame for transmission such that the data block and the HMAC value appear before the hash key in the frame transmission." Although Claim 17 includes different recitations from Claim 1, the Applicants submit that Claim 17 is allowable for at least the reasons presented above. Claims 18-19 are proposed to be allowable as they depend from a valid base claim.

App. No. 10/779,382

Amendment Dated: July 3, 2007

Reply to Office Action of March 12, 2007

Claims 12-15 and 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carro in view of Mache. With regard to Claim 20, the Office Action stated that Carro discloses all of the recitations except that "Carro does not disclose that a counter in the client device that is arranged to provide another count, and a hash function in the client device that is arranged to compute additional hash keys using the count and previously stored hash keys (storing a hash key that is associated with the frame when the RSA signature is verified (the prior art discloses the hash key of the hash function received is being computed to obtain the hash value, therefore, the hash key must have be stored before it can use to decode the hash value))." The Applicants respectfully disagree. Claim 20 recites in part "a broadcast receiver that is arranged to receive a transmitted frame, wherein the transmitted frame includes an HMAC value and a data block, and ends with a hash key S_i ; ... a verification function block that is arranged to verify the hash key (S_i) with the computed hash keys, and also arranged to verify the HMAC value with the hash key (S_i) and the previously stored hash keys; ... and a means for storing the hash key as a previously stored hash key when the frame is accepted such that subsequent frames utilize the stored hash key for verification." For at least the reasons presented above, Claim 20 is proposed to be allowable as presented.

Conclusion

In view of the foregoing amendments and remarks, all pending claims are believed to be allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application,

App. No. 10/779,382

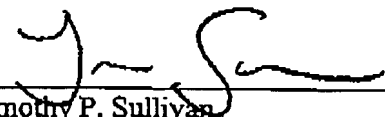
Amendment Dated: July 3, 2007

Reply to Office Action of March 12, 2007

the Examiner is requested to contact the undersigned attorney for the applicant at the telephone number provided below.

Respectfully submitted,

MERCHANT & GOULD P.C.


Timothy P. Sullivan
Registration No. 47,981
Direct Dial: 206.342.6254

MERCHANT & GOULD P.C.
P. O. Box 2903
Minneapolis, Minnesota 55402-0903
206.342.6200

